MANAGEMENT MODEL FOR THE FEDERAL PUBLIC KEY INFRASTRUCTURE

Noel A. Nazario, **William E. Burr**, and **W. Timothy Polk**
Security Technology Group
National Institute of Standards and Technology
NIST North, Room 426
820 West Diamond Avenue
Gaithersburg, MD 20899
NNazario@nist.gov, WBurr@nist.gov, WPolk@nist.gov

Introduction and Background

A Public Key Infrastructure (PKI) is a collection of systems that exist for the purpose of generating, revoking, disseminating, and otherwise managing public key certificates. Public key certificates are signed digital documents that bind the identity of certificate holders to their public keys. The use of public key cryptography is central to the widespread use of electronic signatures and should enable user authentication, message integrity, and message non-repudiation services essential for the general acceptance of electronic commerce and other electronic services. The Federal Government has recognized the potential gains in efficiency and enhanced level of service to the citizen that can be afforded by this technology. The Government also recognizes the potential commercial impact of new online services enabled by the use of public key cryptography. Such recognition has prompted several Government entities to work together to devise an interoperable PKI.

To meet expectations, the Federal PKI has to offer a consistent level of service, reliability, and trustworthiness regardless of which components were involved in the creation and maintenance of a certificate. The Federal PKI needs to interoperate with other infrastructures, be available in an uninterrupted fashion, and maintain its integrity so that it stands up to scrutiny and evidence provided by it is admissible in court. To ensure a robust infrastructure and a consistent level of service, a quality control and management structure is needed. This document describes a proposed management structure for the Federal PKI envisioned by the Federal PKI Technical Working Group (TWG). The TWG has released a Concept of Operations (CONOPS) [6], a Technical Security Policy (TSP) [5], and a Requirements document [4]. The PKI described in those documents assumes the use of the X.509 version 3 certificate format [2] and the management structure discussed in this paper.

Federal PKI Components

The main components of the proposed Federal PKI are Certification Authorities (CAs) and Organization Registration Authorities (ORAs). In addition, the Federal PKI relies on the existence of a Policy Approving Authority (PAA), a Directory Service (DS), PKI Transaction Archives, and the Computer Security Objects Register (CSOR) [8]. Figure 1 shows several CAs, ORAs, PKI Clients, and a Directory. The PAA is a management entity and is therefore not shown here; the CSOR is a service provided externally and is not shown either. Transaction Archives are considered as part of the individual CA installations. The CONOPS identifies other peripheral components that support value-added services, but

are not essential to the proposed Federal PKI.

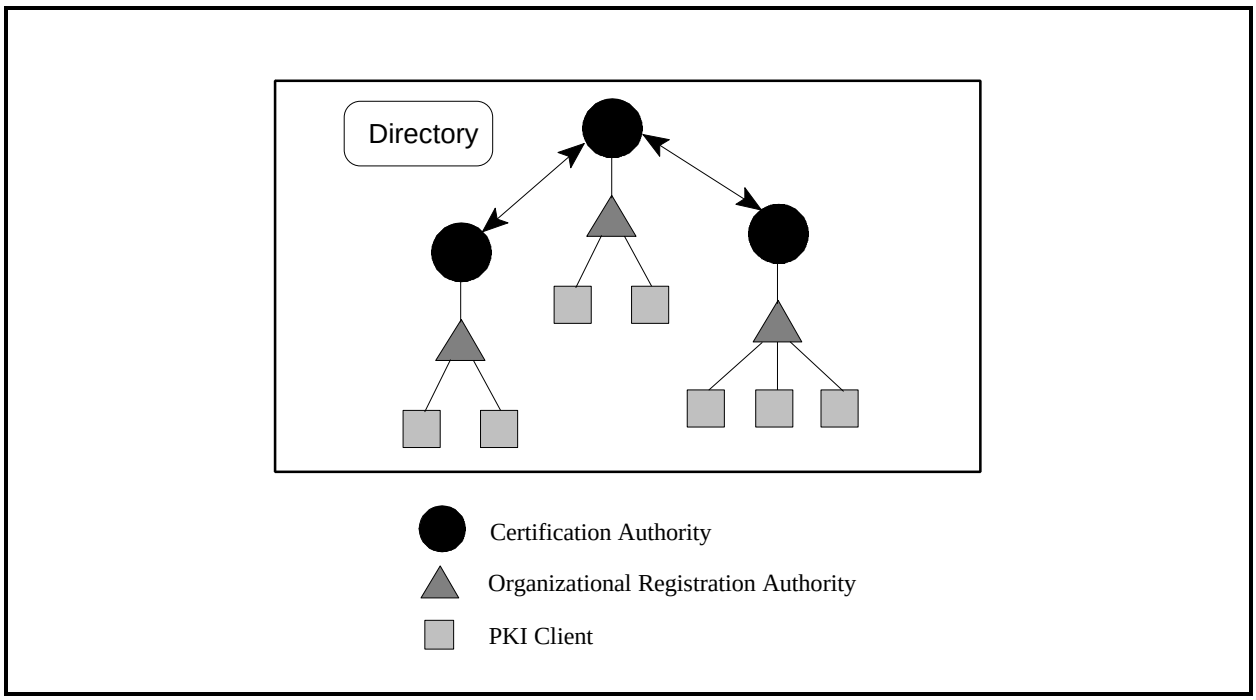

Figure 1 - Main Components of Proposed Federal PKI

While CAs in the proposed Federal PKI are organized hierarchically for practical and administrative reasons, the certification paths may also be traversed as a network. The hierarchical links are provided both by certificates and cross-certificates, while the network links are provided through cross-certificates as defined for version 3 of the X.509 certificate format. Cross-certification refers to the mutual issuing of certificates by two CAs. It implies that both CAs trust the certificates issued by each other. Each CA makes an off-line decision of whether to cross-certify with another based on its knowledge of the policies of the other CA and any other criteria. Cross-certification between CA whose users exhange signed messages frequently makes verification more efficient. As indicated in the CONOPS, trust is delegated hierarchically and most cross-certificates are required to preserve that delegation. Certain special "cross-certificates" can override these restrictions imposed on trust delegation and naming space, but their use is limited to "leaf" CAs that cannot certify subordinate CAs. Since leaf CAs cannot have subordinate CAs, only the users of the cross-certified CAs could be affected by an unwise cross-certification.

Certification Authorities

CAs generate, revoke, publish, and archive certificates. All Federal PKI CAs sign the certificates and CRLs they generate using Federal Information Processing Standard (FIPS) approved digital signature algorithms. CAs may impose name space and policy restrictions on subordinate CAs. All CAs either operate, or are associated with, a directory server. CAs also maintain an off-line log of all transactions. Every CA operates under one explicitly defined CA Operational Policy, but may issue certificates under multiple Certificate Issuance Policies. CA Operational Policies explicitly define the operation of a CA and include: backup procedures, archiving procedures, personnel requirements, functional roles for operators, physical protection, CA cryptographic module requirements, access controls, CA private key handling, etc.

Certificate Issuance Policies state the requirements or constraints under which certificates are issued and include: identification requirements for certification of users and CAs, procedures for generating, storing, revoking, and archiving certificates and key material, etc.

Although the use of cross-certificates allows the Federal PKI to be seen as a network of CAs joined through bilateral trust relationships, it is organized as a hierarchy that roughly follows that of the different departments and agencies of the U.S. Federal Government. That hierarchy delineates trust delegation within the Infrastructure. Trust and name space restrictions imposed by the hierarchy should be preserved by all Federal PKI CAs, with the possible exception of "leaf" CAs. Without this limitation, restrictions imposed on CAs could be ignored and certificates could not be verified consistently depending on the verification path chosen. The CA at the top of the hierarchy is the Root CA. All trust propagates from this CA. The Federal PKI could conceivably have more than one Root CA, each one at the top of the hierarchy for a different segment of the U.S. Government.

Organizational Registration Authorities

The Organizational Registration Authority (ORA) is the function that vouches for the identity of users requesting certification. CA operators and users request initial certification by appearing in person before the ORA for their parent CA and submitting a certificate request. This certificate request consists of a partially complete certificate signed with the private key for the public key being certified. This self-signing of the certificate request is done to verify that the user possesses the complete key pair and to provide an integrity check for the request. The ORA function verifies the personal and affiliation information on the request and the signature according to the requirements for the type of certificate being requested. After the signature and the user's identity are verified, the ORA signs and sends the certificate request to the CA. The ORA function may be either physically removed from the certifying CA or collocated with the CA.

Policy Approving Authority

The Policy Approving Authority (PAA) evaluates CA Operational Policies and Certificate Issuance Policies to assess the overall quality of the certificates issued by each CA. The Federal PKI Technical Security Policy (TSP) [5] provides the basis for that assessment, which is used by the PAA to determine the highest assurance level CAs may assign to the certificates they generate. The PAA may assign one of three hierarchical Federal Assurance Levels defined in the TSP. The PAA is directly associated with the Root CA, but it delegates oversight responsibilities to subordinate authorities. The PAA and its designated subordinates perform periodic reviews of the operational procedures of every CA in the Federal PKI to ensure they meet their own policies.

The PAA identifies and delegates responsibilities to subordinate authorities, limits the depth of the PKI hierarchy, approves the use of Federal Assurance Levels, monitors adherence to CA Operational Policies and Certificate Issuance Policies, and optionally assigns name space constraints to CAs and registers additional policies for use throughout the infrastructure.

Directory Service

The Federal PKI relies on the on-line availability of certificates, certificate revocation lists (CRLs), and other policy information for the validation of public key signatures and establishment of confidentiality-protected communications sessions and messaging applications. The basic mechanism for making that

information available is a directory service provided by one or more interconnected directory servers.

The Federal PKI CONOPS assumes a directory service based on the X.500 Directory [1]. All CAs either operate their own directory server or have access to one. Individual directory servers should be known to and accessible by other directory servers and should operate as components of a distributed service. Read access to directory information is provided to all users upon request while maintaining strict control on write access to avoid unauthorized modification. CRLs, certificates, and policies posted in a directory should be signed using FIPS approved digital signature algorithms.

Computer Security Objects Register

The Computer Security Objects Register (CSOR) [8] administers a segment of the registration authority granted to NIST for the U.S. Federal Government. This register holds definitions of objects used by systems that provide security services, identifies mechanism, and assigns unique identifiers used in specifying these objects. The CSOR assigns object identifiers (OIDs) to computer security objects with the prefix, **csor-pki = {joint-iso-ccitt(2) country(16) us(840) gov(101) csor(3) pki(4)}**. Under the PKI OID prefix there will be a branch for CA Operational Policies **{csor-pki ca-op-policy(0)}**, one for Certificate Issuance Policies **{csor-pki cert-issue-policy(1)}**, and one for Certificate Policies **{csor-pki cert-policy(2)}**.

Policies registered in the CSOR are signed by the entity posting the policy to provide an integrity check. The CSOR does not effect any checks, verifications, or sanctioning of the policies. Only the PAA reviews and sanctions the policies and assurance levels it registers in the CSOR.

Federal PKI Management

The CAs that make up the Federal PKI are organized in a hierarchical fashion for administrative purposes as illustrated in Figure 1. The CA at the top of the hierarchy is known as the Root CA and is associated with the PAA. There may be more than one hierarchy in the Federal PKI, each with a separate root and PAA. The PAA is responsible for the integrity and trustworthiness of a management domain within the Federal PKI. The PAA reviews CA policies and operational procedures to determine the Federal Assurance Levels that may be claimed on certificates created by a CA.

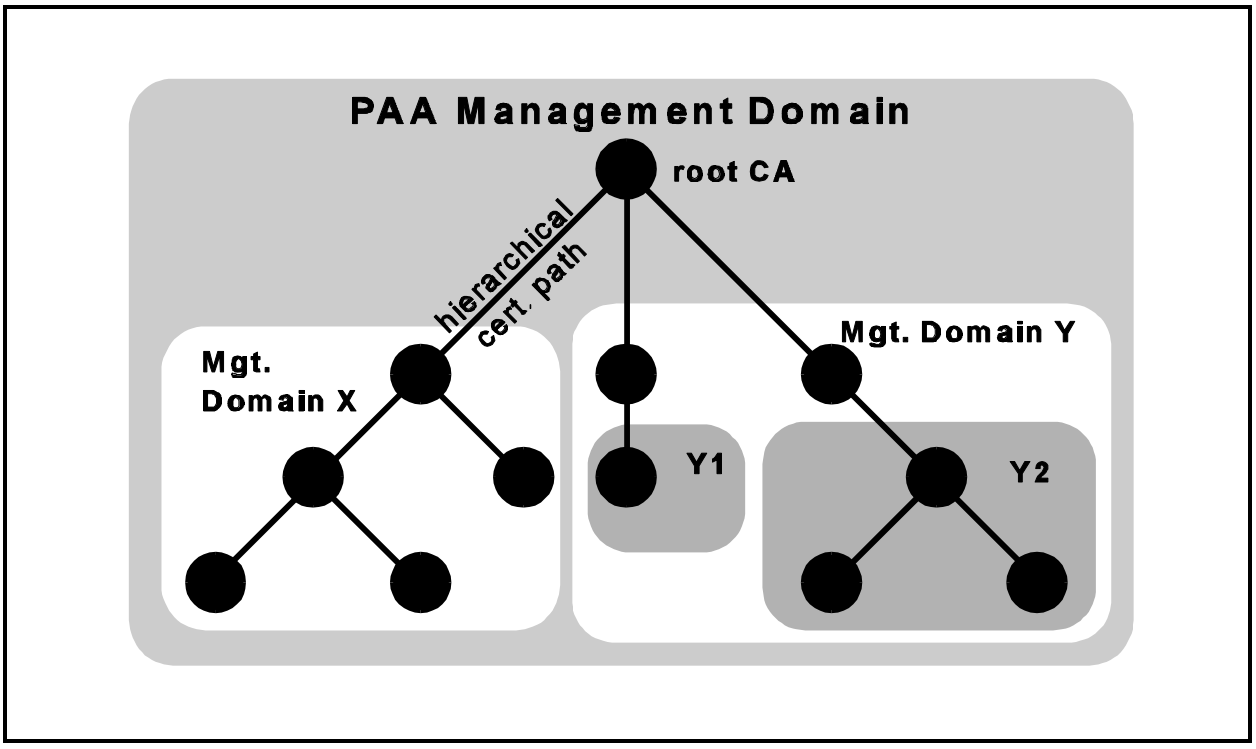

Figure 2 - Proposed PKI Management Domain Nesting

In supervising the operation of the CAs within a domain of the Federal PKI, the PAA will call upon the management entities of several key CAs to perform oversight functions for segments of the domain. Selected management entities may be given oversight responsibilities over more than one CA. The PAA will delegate oversight responsibilities to local authorities selected according to geographical location, expertise, resources, et cetera. The distribution of the oversight responsibilities of the PAA adds flexibility and efficiency while ensuring even levels of quality for the different types of certificates granted by the Federal PKI regardless of the CA creating a certificate.

The lowest level of management responsibilities is local since CAs are mostly autonomous in their operations. The main goal of local management is to implement procedures that meet stated policies. Local management deals with daily operations, it is responsible for the configuration, performance, accounting, fault, and security management of the CAs and their respective ORAs.

Policies

The Federal PKI Technical Security Policy (TSP) defines two types of security policies: CA Operational Policies and Certificate Issuance Policies. CAs operate under one explicitly defined CA Operational Policy, but may issue certificates under several Certificate Issuance Policies depending on the assurance level for the certificate requested. The combination of the CA Operational Policy and the specific Issuance Policy used to authenticate the identity of a certificate holder defines the *certificate policy* identified in the extensions to the X.509 version 3 certificate. The certificate policy, or policies, in the certificate should give the recipient of a signed message enough information to assess the trustworthiness of the binding between the signature and the identity of the sender. Real time evaluation of the actual policies used to issue the signer's certificate and to operate the CAs involved in the signer's certificate chain is too complicated to be efficient and reliable. To avoid that problem, the TSP defines three Federal Assurance

Levels.

A Federal Assurance Level is an indication of the general level of trust that can be placed on a certificate that is uniformly understood throughout the Federal PKI. The assessment of the trustworthiness of the information in a certificate is made by the PAA upon evaluating the policies and procedures followed by the certifying CA. Even though they are not actual policies, Federal Assurance Levels will be conveyed in the
certificate policy extension of Federal PKI certificates. The PAA will register its assurance levels (i.e., low, medium, high) in the CSOR under the certificate policies branch. CAs may assign only one Federal Assurance Level to any certificate.

Restrictions

Since all trust in the Federal PKI is derived from the Root CA, the PAA also plays a role in setting naming and path length restrictions on other CAs. Naming restrictions can be used as a tool in managing the distinguished name space, thus helping to ensure the uniqueness of all user names in the infrastructure. Naming restrictions may also provide a way to establish a logical association between distinguished names, roles, and affiliation of the users or any other useful identification information.

Path length restrictions can be used to limit hierarchical paths to a manageable size (e.g., three levels deep). They are also used to determine when a CA is considered a Leaf CA. Being able to identify a Leaf CA is important since they are allowed to circumvent certain restrictions imposed by the hierarchical path to the root when cross-certifying with other leaf CAs.

CA Assurance Level Assessment

CAs request the PAA to perform an initial assessment of their policies and procedures prior to requesting initial certification. After that initial assessment, the PAA performs periodic reviews of the operations of every CA in the infrastructure to ensure that they maintain conformance with their own policies. As part of this assessment, the PAA determines the Federal Assurance Levels that the CA may include in the certificates it generates according to its CA Operational Policy and the Certificate Issuance Policies it follows. The frequency of the periodic assessments is determined by the PAA.

These assessments are based on the guidelines provided by the TSP and information provided by the CAs. Upon request of the PAA, CAs:

- identify their target Federal Assurance Levels;
- identify the policies followed and where they are posted;
- identify the community or communities they serve;
- identify the equipment,Trusted Computer System Evaluation Criteria [3] or equivalent rating, and FIPS 140-1 [7] rating of the cryptographic modules;
- identify physical and personnel security measures;
- identify the personnel involved in the operation of the CA, their roles, and what training have they received prior to operating the CA;
- identify the directory server, or servers, where they post certificates and certificate revocation lists;
- provide documentation on their operational procedures (including initialization, backup, archive, audit, revocation, etc.);
- provide statistics on number of users and subordinate CAs, number and type of cross-certificates, the volume of transactions, and average load due to revocation processing;
- allow the observation of actual day-to-day operations.

In addition to the documentation identified above, CAs perform the following management functions:

- Maintain a record of certificates it issued;
- Create and maintain system audit logs;
- Archive certificates and CRLs;
- Supervise the operation of remote ORA functions.

The management of the ORAs is the responsibility of their respective CAs, therefore ORA operational procedures should be addressed by CA Operational Policies. Management functions performed by ORAs include:

- Maintain contact information for certificate holders;
- Create and maintain system audit logs.

If a CA or its ORAs fail to implement certificate generation and maintenance procedures in accordance with its posted policies, fail to require appropriate identification information from certificate requesters, or issue certificates identified with Federal Assurance Levels higher than those authorized by the PAA, the CA's certificate and the cross-certificate with its parent will be revoked by the PAA.

Conclusion

A successful Federal PKI has to offer a consistent level of service, reliability, and trustworthiness regardless of which components were involved in the creation and maintenance of a certificate. It should also accommodate security policies that meet the requirements of communities with very different missions and goals. Such an infrastructure needs a management model that provides both uniformity of service and the flexibility to meet special needs.

The proposed management model for the Federal PKI meets these requirements. It defines a central authority that relies on delegation of responsibilities to monitor the operations of the Certification Authorities and ensure that they operate according to policies they claim to enforce. The Policy Approving Authority (PAA) is the central management authority for the Federal PKI. It performs the following functions:

- Evaluates the policies supported by Federal CAs and assigns Federal Assurance Levels according to the criteria in defined in the Federal PKI Technical Security Policy;
- Manages the distinguished name space by establishing naming restrictions;
- Controls the hierarchical depth of the Federal PKI by imposing path length restrictions;
- Periodically evaluates the operation of all CAs in the Federal PKI to determine if they are operating according to their own policies;
- Establishes subordinate management domains and assigns selected local authorities to perform CAs evaluations;
- Determines the frequency of periodic evaluations.

References

1. CCITT X.500 Series (1993) | ISO/IEC 9594,1--9, *Information Technology -- Open Systems Interconnection -- The Directory*, 1995.

2. Draft Amendments to ITU-T Rec. X.509 | ISO/IEC 9594-8, *Information Technology -- Open Systems Interconnection -- The Directory: Authentication Framework*, 30 June 1996.

3. DOD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985.

4. *Federal Public Key Infrastructure (PKI) Technical Specifications (Version 1) - Part A: Requirements*, Federal PKI Technical Working Group, 31 January 1996.

5. *Federal Public Key Infrastructure (PKI) Technical Specifications (Version 1) - Part B: Technical Security Policy*, Federal PKI Technical Working Group, 24 January 1996.

6. *Federal Public Key Infrastructure (PKI) Technical Specifications (Version 1) - Part C: Concept of Operations*, Federal PKI Technical Working Group, 16 November 1995.

7. FIPS PUB 140-1, *Security Requirements for Cryptographic Modules*, January 1994.

8. NISTIR 5308, N. Nazario, *General Procedures for Registering Computer Security Objects*, December 1993.